# Towards Improving Service Accessibility by Adaptive Resource Distribution Strategy

Jinqiao Shi[1,3](✉), Xiao Wang[1,2,3], Binxing Fang[1,3], Qingfeng Tan[1,3], and Li Guo[1,3]

[1] Institute of Information Engineering, CAS, Beijing, China
[2] Institute of Computing Technology, CAS, Beijing, China
[3] National Engineering Laboratory for Information Security Technologies, Beijing, China
{shijinqiao,fangbinxing,tanqingfeng,guoli}@iie.ac.in, wangxiao@nelmail.iie.ac.in

**Abstract.** Along with the rapid development of Internet, accessibility has become one of the most basic and important requirements for Internet service. Service resource, the knowledge that can help users get access to the service finally, is the focus of accessibility confrontation between the adversary and Internet services. Most of current resource distribution strategies adopt the "many access points" design and limit the number of service resources distributed to any user. However, current design is vulnerable to enumeration attack where an adversary can enumerate many service resources under the disguise of many pseudonyms (Sybil identities). To mitigate this challenge, an adaptive resource distribution strategy based on trust management is proposed in this paper. Under this strategy, user's trust is adjusted according to his behavior. Both client puzzle and the resources assigned to the user are dynamically generated according to his trust value. Simulation result indicates that, this strategy can distinguish honest users from adversary Sybils, thus increasing the difficulty for an attacker to enumerate service resources while ensuring access to service for honest users.

**Keywords:** Service accessibility · Resource · Trust management · Resource distribution · Sybil attack

## 1 Introduction

Along with the rapid development of Internet, cyber space has become a new competition field between users, business competitors, or even countries. Therefore, we need to extend the concept of service accessibility, the "ability to access" and benefit from some system, to Internet field, trying to improve users' ability of accessing Internet service under restricted Internet environment. In practice, attacks and defense methods aiming at service accessibility can be found from various areas in both academic and industrial fields. With the help of a DPI system, an adversary can identify its target based on communication relations,


J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 535–540, 2015.
DOI: 10.1007/978-3-319-23829-6_39

communication contents or even communication behaviors between users and Internet services. Once the targets are identified, the adversary can prevent users from accessing them with the help of many effective methods [2]. As for the service provider, proxy is the primary and widely adopted method to fight against this process. To relieve the threats of these new technologies, the adversary has shifted their target from Internet services to the proxy systems.

The accessibility confrontation between the adversary and proxy provider can be viewed as a competition for service resources — the adversary aims to identify them while Internet services try to protect them from being discovered by the adversary. The term "resource" here refers to the knowledge that can help users get access to the service finally, such as IP address, proxy, URL, etc. Though various distribution restrictions [3,6,7] are adopted in the design of proxy systems, these is still a challenging problem in the resource distribution process: the service should make it easy for users to learn enough knowledges while preventing adversaries from enumerating them in the same way. This paper presents an adaptive resource distribution strategy to conquer this challenge. This strategy consists of two component: (i) the trust manage system adjusts users' trust values according to their different behavior modes; (ii) the adaptive resource distribution strategy can assign resources to users and adversary Sybils dynamically according to their trust values. Experiments show the effectiveness of this strategy in improving service accessibility under enumeration attacks.

## 2 Problem Statement and Accessibility Metric

Most real-world systems assign resources to users with some restrictions and principles. For example, anonymous communication systems like Tor [4], JAP [1] and covert communication systems like Infranet [5] have a trusted resource management center. All resources in the system are assigned to users by the centralized distributor with a few restrictions. We summarized the resource distribution problem under enumeration attacks as shown in Fig. 1. There are two types of players: a *distributor*, who acts as a trusted center that knows the complete list of resources and distributes resources to users; *users*, who request and get resources form the distributor. Each user plays the role of either an *honest user* or an *adversary Sybil*. Compared with the honest users, adversary Sybils tend to attack resources they got rather than using them.

The interaction between the system and users contains two phases: **(i) Resource Distribution.** Users send resource request to the distributor and obtain a few resources from it. We use $R = \{r_1, r_2, \cdots\}$ to denote all resource in the system. $R_i = \{r_{i_1}, r_{i_2}, \cdots, r_{i_\omega}\}$ is the resource set $u_i$ gets from the distributor. $\omega$ is a distribution parameter, representing for the number of resources distributed to each user. **(ii) Using or Attacking.** After obtaining resources from the distributor, an honest user will utilize these resources while the adversary will attack them and make them unreachable. As a result, the resource in the system can be divided into two classes: *reachable resources* and *unreachable resources*. Unreachable resources is resources that have been discovered and

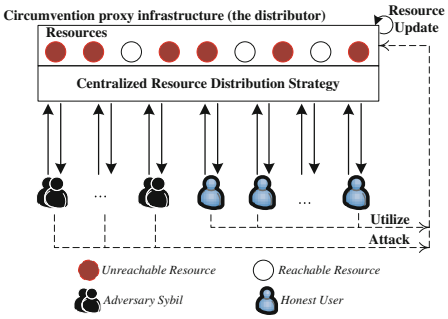


**Fig. 1.** Resource distribution under enumeration attack

blocked by the adversary. Only reachable resources can help users get access to the service.

Accessibility is the ability to get access to the service. Actually, an honest user $u_i$'s availability of accessing the system depends on the reachability of resources he gets from the distributor. Let $P_{r_i}$ to denote the probability that there exists at least one reachable resource in $R_i$. Then, from the perspective of the honest user $u_i$, accessibility of the infrastructure can be given by (1).

$$Acc(u_i) = 1 - \prod_{j=1}^{\omega} (1 - P_{r_{i_j}}), \qquad r_{i_j} \in R_i \tag{1}$$

From the equation we can observe that, accessibility improvement and enumeration-resistance is two conflicting goals for resource distribution strategies that treat honest users the same way with Sybils.

## 3 Adaptive Resource Distribution on Trust Management

### 3.1 Strategy Overview

To tackle the challenges presented above, we presented an adaptive resource distribution strategy based on trust management in Fig. 2. As shown in the figure, this strategy consists of two components:

- Trust Management. Trust management is the basis of the proposed adaptive resource distribution strategy. It assigns a trust value to each user and update this value dynamically according to that user's behaviors.
- Adaptive Resource Distribution. The adaptive resource distribution component assigns different resource to different users according to their trust values.

**Trust Management.** Trust management component consists of two basic functions: trust initialization and trust update. The initial trust value of the new user is determined by the trust values of users who invite him. And trust management

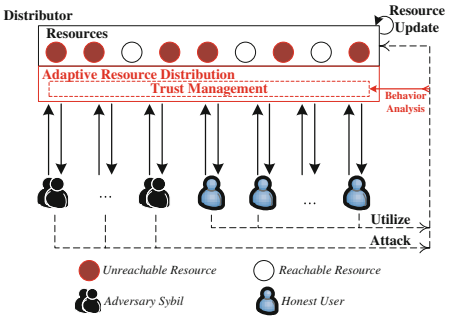


**Fig. 2.** Adaptive resource distribution strategy based on trust management

component also updates their trust values according to users' behaviors. It can distinguish honest users from Sybils by their trust values, i.e., the trust values of honest users should be higher than that of attacker pseudonyms,

**Adaptive Client Puzzle.** The ultimate goal of adaptive client puzzle is to justify the price of resource request: providing honest users an easy puzzle while giving attacker Sybil a hard one.

**Adaptive Resource Selection.** The possibility of a user receiving reachable resources is positively correlated with its trust, thus limiting adversary's enumeration attack while ensure accessibility for honest users.

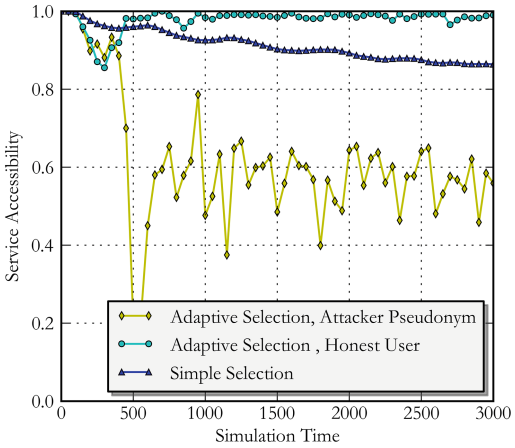


**Fig. 3.** Comparing traditional resource distribution and adaptive resource distribution

## 4 Accessibility Evaluation

We simulated the proposed adaptive resource distribution strategy as well as a classic traditional resource distribution strategy. The service is supposed to have been running for a long time before adopting our strategy. We set the adversary Sybil percentage to be 10 %, i.e., 10 % of users in this system is adversary Sybils, leaving 90 % to be honest. Figure 3 compares the traditional resource distribution strategy with adaptive resource distribution from the aspect of accessibility. When using a random resource distribution strategy, the probability of receiving reachable resource is the same for both honest users and adversary Sybils. However, under the adaptive resource distribution strategy, honest user can get a higher accessibility than adversary Sybils. Furthermore, the accessibility of honest users under the proposed strategy is higher than that under traditional distribution strategy; and the accessibility from Sybil's view under the proposed strategy is much lower than that under random resource distribution strategy. Figure 3 validated the effectiveness of the proposed strategy: it can improve service accessibility for honest users while relieving adversary's enumeration attack.

## 5 Conclusion and Future Work

Based on the analysis of traditional resource distribution strategies, this paper proposed a model and formalization of the resource distribution problem. In order to further improve accessibility, an adaptive resource distribution strategy based on trust management is proposed. Simulation results show the effectiveness and wide applicability of this strategy in improving the accessibility of Internet services under enumeration attacks.

**Acknwoledgement.** This work is supported by National Natural Science Foundation of China (Grant No.61100174), National Key Technology R&D Program (Grant No.2012BAH37B04) and Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No.XDA06030200).

## References

1. Berthold, O., Federrath, H., Köpsell, S.: Web MIXes: a system for anonymous and unobservable internet access. In: Federrath, H. (ed.) Designing Privacy Enhancing Technologies. LNCS, vol. 2009, pp. 115–129. Springer, Heidelberg (2001)
2. Deibert, R.: Access denied: The practice and policy of global internet filtering. The MIT Press (2008)
3. Dingledine, R., Mathewson, N.: Design of a blocking-resistant anonymity system. Technical report (2006)
4. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: Proceedings of the 13th conference on USENIX Security Symposium, vol. 13, pp. 21–21. USENIX Association (2004)

5. Feamster, N., Balazinska, M., Harfst, G., Balakrishnan, H., Karger, D.: Infranet: Circumventing web censorship and surveillance. In: Proceedings of the 11th USENIX Security Symposium, pp. 247–262. USENIX Association, Berkeley (2002)
6. Feamster, N., Balazinska, M., Wang, W., Balakrishnan, H., Karger, D.R.: Thwarting web censorship with untrusted messenger discovery. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 125–140. Springer, Heidelberg (2003)
7. Köpsell, S., Hillig, U.: How to achieve blocking resistance for existing systems enabling anonymous web surfing. In: Proceedings of the 2004 ACM workshop on Privacy in the electronic society, pp. 47–58, WPES 2004. ACM, New York (2004)